THE HONORABLE JAMES L. ROBART

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STACY PENNING, SUNGGIL HONG, LAURA BONETTI, JONATHAN FINESTONE, TANISHA DANTIGNAC, and ROBERT MASON, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

MICROSOFT CORPORATION,

Defendant.

Case No. 2:25-cv-00570-JLR

DEFENDANT MICROSOFT CORPORATION'S MOTION TO DISMISS

NOTED ON MOTION CALENDAR: July 21, 2025

ORAL ARGUMENT REQUESTED

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

Plaintiffs' Complaint is one of many across the country seeking to apply antiquated privacy and wiretapping statutes to cover routine online practices that these laws were never intended to regulate. Plaintiffs allege they visited websites that used Microsoft's "advertising and analytics platform, Xandr, and its Adnxs Pixel" and "Bing Pixel."[1] *See* Dkt. 1 ("Compl.") ¶ 1, 56–68. They allege that Microsoft collected, for advertising purposes, information about their devices, browsers, Internet Protocol ("IP") addresses, and the uniform resource locators ("URLs") of websites they visited. *See id.* ¶¶ 231–302. Based on these allegations, Plaintiffs allege claims, on behalf of themselves and nationwide and California putative classes, for (1) intrusion upon seclusion under California law, (2) violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631(a) (wiretapping), (3) violation of CIPA, Cal. Penal Code § 638.51(a) (installation or use of a pen register), (4) unjust enrichment under California law, and (5) violation of the federal Wiretap Act (the "Wiretap Act"), 18 U.S.C. § 2511(1)(a) (interception of communications).

Plaintiffs assert these claims even though, as they admit, the information Microsoft allegedly collects is not associated with individual identity (e.g., a name) but rather with a random "ID number" generated by Microsoft. *See* Compl. ¶ 126. Moreover, Microsoft expressly requires its customers—here, the websites Plaintiffs allegedly visited—to comply with privacy laws. *See, e.g.*, Microsoft, Microsoft Advertising Agreement (last visited June 23, 2025). And Plaintiffs do not allege that these services in any way violate the privacy regimes, such as the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.100, *et seq.*,[2] that actually

[1] There is no Microsoft service called the "Bing Pixel." Based on the allegations in the Complaint, Microsoft assumes Plaintiffs are referring to Microsoft's Universal Event Tracking ("UET") service. Additionally, the proper defendant as to the Adnxs Pixel and the Xandr service is Xandr, Inc., not Microsoft Corp. Finally, many of Plaintiffs' allegations about how pixels and cookies work, among others, are grossly factually inaccurate. For purposes of the motion to dismiss, however, Microsoft accepts Plaintiffs' allegations as true, as it must under Rule 12(b)(6).

[2] The CCPA is California's comprehensive privacy statute, which includes detailed requirements related to the collection, retention, and sale of personal information, including for third party advertising purposes.

regulate the collection and use of personal information online.[3] In fact, all the websites Plaintiffs allegedly visited within the relevant time period publicly disclose that browsing activity would be shared with third parties for advertising purposes, and Plaintiffs do not allege that they took any widely available measures to avoid the websites' use of pixels and cookies such as blocking them through their browser. The Court should not allow Plaintiffs to stretch common-law privacy and wiretap laws beyond their intended scope, and it should dismiss the Complaint with prejudice for the following reasons:

First, Plaintiffs cannot allege "concrete harm," and therefore lack Article III standing, because they base their claims on Microsoft's alleged collection, use, and disclosure of website browsing information, which is "not the type of private information that the law has historically protected." *See Popa v. PSP Grp., LLC*, No. C23-0294, 2023 WL 7001456, at *4 (W.D. Wash. Oct. 24, 2023) (Robart, J.). Nor can they establish standing to pursue claims based on websites they did not visit and technologies they did not encounter. *See Simon v. E. Ky. Welfare Rts. Org.*, 426 U.S. 26, 40 n.20 (1976) (citation omitted).

Second, Plaintiffs do not state a claim for intrusion upon seclusion under California law because the public websites they visited within the relevant time period *all* disclosed that they collected and shared information for third-party advertising—activity the CCPA expressly permits. This defeats Plaintiffs' claim—which they cannot assert on a nationwide basis in any event—that they had a reasonable expectation of privacy, let alone experienced any highly offensive breach of privacy norms.

Third, Plaintiffs' wiretapping claims under the federal Wiretap Act and CIPA fail because Plaintiffs do not plausibly allege that Microsoft intercepted the contents of communications, much less that it did so while the alleged communications were "in transit."

[3] Recognizing this, the California Senate recently unanimously passed Senate Bill 690 ("SB 690") "to protect businesses from vexatious litigation" under CIPA targeting online advertising technologies already regulated by the CCPA. *See* Analysis of SB 690, Sen. Comm. on Pub. Safety, 2025-2026 Reg. Sess. (Cal. Apr. 25, 2025).

Fourth, Plaintiffs fail to state a claim under California's pen register statute, which applies to information about person-to-person communications, like phone calls, *not* browsing activity on publicly available sites.

Fifth, because the Wiretap Act and CIPA are criminal statutes carrying severe penalties, the Court should apply the rule of lenity, which provides that only conduct clearly covered by the statutory text can give rise to criminal liability and which requires resolving any ambiguity in Microsoft's favor. *See United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012).

Sixth, Plaintiffs' claim for unjust enrichment cannot proceed, as such a standalone claim does not exist under California law (and cannot be asserted on a nationwide basis anyway), Microsoft has no relationship with Plaintiffs that could give rise to a quasi-contract claim, Microsoft's business practices are not "unjust," and Plaintiffs do not claim that they lack a sufficient remedy at law.

Finally, all Plaintiff Robert Mason's claims are time barred. Plaintiff Mason alleges that he visited the relevant website that deployed Microsoft's technology in February 2021, outside the applicable one to two year limitations periods for his claims.

BACKGROUND

I. Legislative History

The wiretapping statutes on which Plaintiffs base their Complaint became law before the Internet existed; these statutes regulate person-to-person communications, not online advertising. The federal Wiretap Act, passed in 1968, initially "regulated only the 'aural acquisition of the contents of any wire or oral communication.'" *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1103 (9th Cir. 2014). California enacted CIPA in 1967 to "replac[e] prior laws that permitted the recording of telephone conversations with the consent of one party to the conversation." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 768–69 (2002). The Wiretap Act and CIPA permit wiretapping

telephone communications either with consent or after obtaining a court order, among other exceptions. *See* 18 U.S.C. §§ 2511(1)(c), 2516; Cal. Penal Code §§ 631(a), 629.52.

Congress and the California legislature updated these laws to cover electronic forms of communication, but their focus remained on person-to-person communications content. For example, when California passed its pen register statute in 2015 to provide law enforcement with a mechanism to obtain pen registers for ongoing criminal investigations, it largely mirrored the definitions, text, and structure of the federal pen register statute first passed in 1987. *See* A.B. 929, 2015-2016 Reg. Sess. (Cal. 2015); 18 U.S.C. § 3121 *et seq.* Critically, the California legislature did not include any language in the statute suggesting it applied to internet tracking services that were ubiquitous at the time, instead focusing on the collection of information related to, but not consisting of, the "contents of a communication." *See* Cal. Penal Code § 638.50(b) (defining "pen register").

Recently, perhaps motivated by these statutes' statutory damages provisions, *see* 18 U.S.C. § 2520; Cal. Penal Code § 637.2, plaintiffs' attorneys have filed hundreds and hundreds of lawsuits attempting to expand these criminal laws to technologies that analyze "users' interactions with consumer websites." *Popa*, 2023 WL 7001456, at *1. In response, the California Senate unanimously passed amendments to CIPA, clarifying that it does not apply to routine, commercial services like those at issue here. *See* Sen. Bill No. 690, 2025-2026 Reg. Sess. (Cal. Mar. 24, 2025) (as amended) (CIPA's private right of action "does not apply to the processing of personal information for a commercial business purpose"). The Senate did so because CIPA was "never intended to apply" to "website analytics or online advertising," which "are already governed by the . . . CCPA." SB 690 Analysis, Sen. Comm. on Pub. Safety, 2025-2026 Reg. Sess. (Cal. Apr. 25, 2025). The bill is now awaiting passage by the California Assembly.

II. The Xandr and Microsoft Services Alleged in the Complaint.

A pixel is a piece of online technology "that website operators can integrate into their websites." Compl. ¶ 50. Plaintiffs allege they visited websites with the Adnxs pixel or (in one case) the UET pixel on them. *Id.* ¶¶ 231–302. They allege that when a website visitor reaches a website that incorporates one of these pixels, the pixel sends data in the form of a "cookie" to the website visitor's browser, which allows Microsoft to link disparate website browsing sessions associated with that same browser. *Id.* ¶¶ 57, 74–75*; see also, e.g.*, ¶ 162. Plaintiffs claim that, through the operation of these pixels and cookies, Microsoft collected information about their website activities, such as which browser they used, what kind of device they had, their IP address (i.e., a "set of numbers assigned to a device on a network"), and the URLs of websites they visited. *See id*. ¶¶ 61, 234, 248, 258, 262, 273, 282, 296.[4]

Plaintiffs do not allege that Microsoft or the websites they visited made or broke any promises about data collection, that Plaintiffs attempted to prevent cookies from being installed on their browsers, that any party used Plaintiffs' website browsing information for malicious purposes, or that Microsoft offered online advertising services in a manner inconsistent with the CCPA.[5]

Plaintiffs conclude that their website browsing constituted "communications," and they assert that the Xandr and UET pixels "intercepted" those communications, "primar[ily]" by allegedly collecting URLs. *Id*. ¶¶ 61, 64. Alternatively, they claim Microsoft installed "pen

[4] Although they also allege that Microsoft *can* collect information about use of Microsoft branded applications (Compl. ¶ 55) and use of mobile applications (*id*. ¶¶ 95–114), Plaintiffs do not allege that they used any Microsoft branded applications or any mobile applications that used UET or Xandr services. Similarly, although Plaintiffs allege that Microsoft could collect e-mail addresses (*id*. ¶ 116) and location information (*id*. ¶ 117), and later mention in passing that the pixels collected "geolocation," the allegations about Plaintiffs' own experiences do not mention these data elements. *Cf. id.* ¶¶ 231-302.

[5] All browsers offer tools to stop or clear cookies, *see, e.g.*, Compl. ¶ 43, and the CCPA requires websites to, in certain circumstances, provide consumers the right to opt out of certain disclosures of their personal information. Cal. Civ. Code §§ 1798.120, 1798.135. Plaintiffs do not allege they attempted to prevent or delete cookies or were denied their rights under the CCPA.

registers" by allegedly collecting Plaintiffs' "IP address, geolocation, device information, and other persistent identifiers." *Id.* ¶¶ 61, 347.

Plaintiffs also allege that, through data collected via the Adnxs and UET pixels, Microsoft assigns to individuals advertising segments based on their web activity, which Microsoft customers can use to sell advertising space on their websites, bid on available advertising space (i.e., "real-time bidding"), and tailor their advertising campaigns to visitors' interests. *See id.* ¶¶ 202, 135–158. Plaintiffs otherwise vaguely accuse Microsoft of maintaining "profiles" on individuals but do not explain what "profiles" are. *See id*. ¶¶ 236, 250, 260, 271, 283, 298.

Finally, Plaintiffs allege that Microsoft engages in "cookie syncing" with third parties, whereby third-party providers of "Partner Pixels" deployed on the same websites as the Xandr and UET pixels can check if Microsoft already has a cookie corresponding to the visiting browser or IP address, along with other information. *Id.* ¶¶ 39–40, 52, 128, 220–30.

III. Plaintiffs' Allegations

Making largely cookie-cutter allegations, Plaintiffs each allege that Microsoft collected their data when visiting various websites, supposedly "identified" and "profiled" them, and allegedly shared this information with third parties. *Id*. ¶¶ 159–219, 231–302. But by Plaintiffs' own allegations, the only data that Microsoft purportedly collected from Plaintiffs were their ***IP addresses, information about their devices and browsers, and the URLs of pages they visited***. *Id*. As to sharing their data and "identifying" Plaintiffs, Plaintiffs claim that Microsoft shared these same basic data elements with other businesses ("Partner Pixels") after assigning a random "Microsoft ID*"* to them. *See id.*; *see also id*. ¶¶ 119–134 (describing IDs "assign[ed]" to records of web and app activity). And Plaintiffs do not otherwise define or describe the "profiles" that Microsoft allegedly created based on this limited information.

For example, Mr. Penning alleges Microsoft collected his IP address, device and browser information, and URLs of the pages he visited on the Buzzfeed website, which allegedly incorporated the Adnxs pixel, in December 2024. Compl. ¶ 231. Mr. Hong alleges similar collection on the AliExpress website. *Id*. ¶ 241. Ms. Bonetti, Mr. Finestone, and Mr. Mason make similar allegations regarding the Bon Appetit, Hyatt, and Plushcare websites, respectively. *See id.* ¶¶ 255, 277, 289. Ms. Dantignac alleges similar data collection on the Expedia website, but via the Bing Pixel. *See id.* ¶¶ 266-76. Each Plaintiff alleges that Microsoft also provided cookie syncing services to various Partner Pixels on at least some of those websites. *See, e.g.*, *id.* ¶¶ 246, 259, 294. Notably, although Mr. Mason generally claims collection of "information about his medical condition and treatment" when he visited the Plushcare website in February 2021, he alleges only that a *third party*, Criteo, collected this information, not Microsoft. *See id.* ¶¶ 290–91; *see also id.* ¶¶ 217–18.

ARGUMENT

I. THE COURT SHOULD DISMISS THE COMPLAINT FOR LACK OF STANDING

Plaintiffs do not allege an "injury in fact" sufficient to confer Article III standing. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (citations omitted). An injury in fact must be "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Id.* at 339–40 (citations omitted). Mere violation of a statute is not enough. *See TransUnion LLC v. Ramirez*, 594 U.S. 413, 427 (2021). Courts must assess whether an alleged injury "has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *Id.* at 424 (citation omitted).

Plaintiffs claim injury from the alleged collection of IP addresses, device/browser information, and URLs in the form of (i) "dissemination and/or misuse" of their "sensitive, confidential communications and information," and (ii) deprivation of their "right to visit and interact with various internet sites without being subjected to highly intrusive surveillance." *See*

Compl. ¶ 316. But as this Court rightly recognized in *Popa v. PSP Group LLC*, these types of privacy harms do not bear a close relationship to those that traditionally provided a basis for federal jurisdiction. 2023 WL 7001456, at *4; *see also Cook v. GameStop, Inc.*, 689 F. Supp. 3d 58, 66 (W.D. Pa. 2023) (similar). The information at issue here is even less extensive than the "mouse movements, clicks, keystrokes . . . [and] URLs" found insufficient in *Popa* and *Cook.* As courts have repeatedly held, there is no privacy interest in IP addresses and URLs, and device or browser information is no different. *See Khamooshi v. Politico LLC*, No. 24-cv-07836, 2025 WL 1408896, at *3 (N.D. Cal. May 13, 2025) (IP addresses); *Saeedy v. Microsoft Corp.*, No. 23-cv-1104, 2023 WL 8828852, at * 4 (W.D. Wash. Dec. 21, 2023) (URLs); *see also Gabrielli v. Insider, Inc.*, No. 24-cv-01566, 2025 WL 522515, at *8 (S.D.N.Y. Feb. 18, 2025) (dismissing pen register claim on standing grounds and explaining that California's pen register statute "does not codify a substantive privacy right"); *Jones v. Bloomingdales.com, LLC*, 124 F.4th 535, 539 (8th Cir. 2024) (joining "the overwhelming number of district courts to hold that plaintiffs lack standing in [internet tracking] cases like these where they don't allege the interception of private information").

Plaintiffs' speculation that URLs could reveal sensitive information, such as "travel information and health information," *see* Compl. ¶ 66, does not establish Article III jurisdiction. Information about flight or hotel bookings—the type of information supposedly captured during Ms. Datignac and Mr. Finestone's online browsing[6]—are not historically protected as private information, especially when this information is not associated with identifying information. *See, e.g.*, *Lightoller v. Jetblue Airways Corp.*, No. 23-CV-00361, 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023) (alleged collection of browsing activity on a flight-booking website presented no traditional privacy injury). And Mr. Mason does not allege that Microsoft collected his health

[6] The Complaint generally alleges that URLs on Expedia, the website Ms. Dantignac visited, can contain hotel booking dates. *See* Compl. ¶ 65. But Ms. Dantignac alleges she "booked a flight" on Expedia, not a hotel room. *Id*. at ¶ 267.

information—that information was allegedly collected by *Criteo*—not Microsoft. *See id.* ¶¶ 290–91; *see also id.* ¶¶ 217–18.

Further, Plaintiffs do not allege that Microsoft identified them personally, as necessary to claim a privacy injury. *See Mikulsky v. Noom, Inc.*, No. 23-CV-00285, 2024 WL 251171, at *4 (S.D. Cal. Jan. 22, 2024) ("The disclosure of non-individually identifiable data is insufficient to give rise to an injury-in-fact to support Article III standing."); *Massie v. Gen. Motors LLC*, No. CV 21-787, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2022) (similar); *see also U.S. Dept. of Just. v. Reps. Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989). Plaintiffs do not "allege that [they] entered any personally identifiable information" into any of the relevant websites, or that Microsoft was "able to connect the information . . . to [their] identity." *Popa*, 2023 WL 7001456, at *5; *see also Cook*, 689 F. Supp. 3d at 66 (similar). Instead, "everything [plaintiffs] did on [the relevant] website[s]" was effectively "anonymous." *Cook*, 689 F. Supp. 3d at 66. This "dooms any attempt to establish a concrete injury in fact." *Id.* at 66 n.1; *see also Cahen v. Toyota Motor Corp.*, 717 F. App'x 720, 724 (9th Cir. 2017) (no standing because plaintiffs failed to plead how "collection and storage of non-individually identifiable driving history and vehicle performance data cause an actual injury").

Nor can Plaintiffs maintain Article III standing based on allegations that Microsoft "deanonymizes" data by providing "identity resolution" or "cookie syncing" services to third parties. As the Complaint puts it, a website operator "does not (and cannot) know which user[s] visit" its website. *See* Compl. ¶ 41. The fact that, as the Complaint describes, a third party can match a random identifier (e.g., "userABC") to another random identifier, (e.g., "user 123") makes no difference because these random identifiers do not reveal who Plaintiffs are. *See, e.g.*, *id.* ¶ 42. Nonetheless, Plaintiffs suggest that grouping anonymous information with more anonymous information somehow "prevent[s] users from being anonymous when they visit websites." *Cf. id.* ¶ 45; *see also* ¶¶ 119-134 (describing "identity resolution" services that tie

together separate instances of browsing online, but do not attach that browsing to any real-world identity). On its face, this makes no sense—and indeed, Plaintiffs do not explain how the cookie IDs that Microsoft and third parties "assign" to the data they allegedly collect identifies Plaintiffs. *Id.* ¶ 40; *see also Low v. LinkedIn Corp.*, No. 11-CV-01468, 2011 WL 5509848, at *3 (N.D. Cal. Nov. 11, 2011) (no standing where "Plaintiff has not alleged *how* third party advertisers would be able to infer Low's personal identity from LinkedIn's anonymous user ID combined with his browsing history"). And even if Plaintiffs' theory could stand—and it does not—it says nothing about *them* and *their* experiences, and so does not establish Article III standing. *See Ramirez*, 594 U.S. at 431 (explaining that "Article III does not give federal courts the power to order relief to any uninjured plaintiff, class action or not") (citation omitted).

Plaintiffs' "profiling" allegations fare no better, particularly since Plaintiffs do not even attempt to explain what they mean when they use this term. In any event, this case is unlike cases pre-dating *Ramirez*, where the creation of profiles of "*personally identifiable* browsing history" sufficed to establish Article III standing because that information was tied to Facebook profiles that revealed individuals' actual names and real-world identities. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F. 3d 589, 596–99 (9th Cir. 2020) (addressing allegations that the relevant cookie stored the user's Facebook "login ID") (emphasis added); *see also Popa*, 2023 WL 7001456, at *5 (distinguishing *In re Facebook* on this ground). Plaintiffs do not allege any supposed "profile" created by their website browsing activity was linked to a personally identifying profile of theirs on another site, like Facebook.

Plaintiffs also lack standing to pursue claims based on websites they did not visit. *Cf. Simon*, 426 U.S. at 40 n.20. They describe visiting six websites, yet they seek to attack Microsoft for "millions" of other, unidentified websites' alleged use of Microsoft's services. *Id.* ¶ 220; *see also id.* ¶¶ 95–114 (describing Microsoft services allegedly used on "mobile apps [and] devices"). Courts routinely dismiss such claims at the motion to dismiss stage. *See Lozano v.*

Bowmar Nutrition, LLC, No. 21-cv-04296, 2021 WL 4459660, at *3 (C.D. Cal. Aug. 19, 2021) ("Even if Plaintiff has standing to predicate her claims on substantially similar unpurchased products, Plaintiff here pleads no facts indicating the unpurchased products are substantially similar to the [products] she did."). A different result would subject Microsoft—and potentially "millions" of third-party websites—to costly discovery into the technical functioning of websites across the Internet, without any plausible allegations that the websites function similarly, or have similar disclosures to, the six described in the Complaint. *See also Walsh v. Microsoft Corp.*, 63 F. Supp. 3d 1312, 1317–18 (W.D. Wash. 2014) (plaintiffs "lack standing to pursue claims based on products they did not purchase"); *Lee v. Am. Nat'l Ins. Co.*, 260 F.3d 997, 1002 (9th Cir. 2001) (rejecting Plaintiffs' ability to pursue claims where he "did not buy" a product from a particularly entity and therefore "did not suffer any injury due to [that entity's] conduct").

II. THE COURT SHOULD DISMISS THE COMPLAINT FOR FAILURE TO STATE A CLAIM

Plaintiffs must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). This requires "pleading factual content" that permits a "reasonable inference" of liability. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The Court need not accept as true "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *Seven Arts Filmed Ent., Ltd. v. Content Media Corp. PLC*, 733 F.3d 1251, 1254 (9th Cir. 2013).

A. Plaintiffs Fail to Plead Intrusion Upon Seclusion.

To support this claim under California law, Plaintiffs must plead that (1) Microsoft "intentionally intrude[d] into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy," and (2) the intrusion "occur[red] in a manner highly offensive to a reasonable person." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009). This

is a "high bar" that Plaintiffs have not met. *See Belluomini v. Citigroup, Inc.*, No. CV 13-01743, 2013 WL 3855589, at *6 (N.D. Cal. July 24, 2013).[7]

1. Plaintiffs Do Not Plead a Reasonable Expectation of Privacy.

California law presumes that websites may track users for purposes of targeting ads. The CCPA, for example, which regulates what data websites can track and collect, allows online data collection and sharing with third parties for advertising with notice and an *opt out*; it generally does not require consent. *See* Cal. Civ. Code. § 1798.120 (providing consumers the right to opt out of the selling or sharing of their personal information); *id.* § 1798.135 (establishing acceptable opt-out mechanisms and prohibiting businesses from selling or sharing personal information after a consumer opts out)*; see also* § 1798.99.80(c) (implementing rules for "data brokers" who "collect[] and sell[] to third parties the personal information of a consumer with whom the business does not have a direct relationship"). Plaintiffs do not allege otherwise. Because California law permits and regulates the data practices at issue, Plaintiffs cannot plausibly allege an expectation of privacy.[8]

Additionally, privacy policies posted on each of the websites at issue disclose that browsing information will be tracked and shared with third-party advertising partners and networks.[9] In the face of these disclosures, Plaintiffs cannot plausibly allege that they reasonably expected that their browsing activity would be kept private. *Lloyd v. Facebook, Inc.*, No. 23-15318, 2024 WL 3325389, at *2 (9th Cir. July 8, 2024) (plaintiff "did not have a reasonable expectation of privacy" where "data policy g[ave] clear notice that third party partners may share data"). This would be true even absent those disclosures, as courts recognize that "internet

[7] Plaintiffs cannot state a claim for intrusion upon seclusion under California law on behalf of non-California residents, because California common-law does not apply extraterritorially.

[8] The CCPA imposes additional requirements regarding "sensitive personal information," which includes "[p]ersonal information collected and analyzed concerning a consumer's health." Cal. Civ. Code § 1798.135(ae)(2)(B). However, no Plaintiff alleges that Microsoft collected and analyzed this information.

[9] *See* Declaration of Nicola Menaldo, ¶¶ 2–13 & Exs. A–F. Plaintiffs' Complaint analyzes the relevant websites in detail. The Court therefore can consider privacy policies publicly posted on those websites. *See, e.g.*, *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005); *Opperman v. Path, Inc.*, 84 F. Supp. 3d 962, 976 (N.D. Cal. 2015) (taking judicial notice of publicly available privacy policies relevant to plaintiffs' claims).

browsing involves the collection of users' data, including by tracking users across the internet, *and a reasonable user should expect as much.*" *Hubbard v. Google LLC*, No. 19-cv-07016, 2024 WL 3302066, at *7 (N.D. Cal. July 1, 2024) (collecting cases); *Thomas v. Papa Johns Int'l, Inc.*, No. 22-CV-2012, 2024 WL 2060140, at *2 (S.D. Cal. May 8, 2024) (similar); *see also United States v. Forrester*, 512 F.3d 500, 509–10 (9th Cir. 2008) ("Internet users have no expectation of privacy in . . . the IP addresses of the websites they visit."); *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1190 (N.D. Cal. 2020) (similar).

On this basis, alone, the Court should dismiss their invasion of privacy claim. *See Thomas*, 2024 WL 2060140, at *2 (joining "a number of courts" that "have found that consumers do not have a reasonable expectation of privacy" in internet browsing activity) (collecting cases); *see also Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012).

2. Plaintiffs Do Not Allege Highly Offensive Conduct.

Plaintiffs must also allege an invasion that is "sufficiently serious" to constitute "an *egregious breach* of the social norms underlying the privacy right." *Hill v. Nat'l Collegiate Althetic Ass'n*, 7 Cal. 4th 1, 26, 37 (1994) (citations omitted).

Plaintiffs argue that Microsoft's business practices are highly offensive because Microsoft allegedly (1) collects internet browsing activity, (2) combines that information to create profiles, and (3) sells those profiles for advertising. *See* Compl. ¶ 320. But even if Plaintiffs' allegations were correct—which Microsoft does not concede—they do not state a claim for intrusion upon seclusion because the California legislature has declined to prohibit these practices, adopting a mostly opt-*out* regime. *See supra* at 12. It also treats information used "to create a profile" about a consumer as ordinary "personal information." *See* Cal. Civ. Code § 1798.140(v)(1) & (v)(1)(K) (defining "personal information"). Conduct that the California legislature allows subject to regulation cannot be highly offensive as a matter of law. *See Hernandez*, 47 Cal. 4th at 292.

At bottom, Plaintiffs' Complaint targets "routine commercial behavior" akin to "obtaining [a person's] address without his knowledge or permission" to "mail [that person] coupons and other advertisements." *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992–93 (2011), *as modified* (June 7, 2011). This is not an egregious breach of social norms. *See also In re Google, Inc. Priv. Pol'y Litig.*, 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014) (courts "have consistently refused" to find a "serious or egregious violation[] of social norms" in "disclosure of common, basic digital information to third parties"); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (disclosing "unique device identifier number, personal data, and geolocation information" was not "an egregious breach of social norms"). Plaintiffs' failure to plead highly offensive conduct by Microsoft also requires dismissing this claim. *See Hubbard*, 2024 WL 3302066, at *8.

B. Plaintiffs Fail to Allege Unlawful Wiretapping under the Wiretap Act or CIPA.

To plead a Wiretap Act claim, Plaintiffs must allege that Microsoft "(1) intentionally (2) intercepted (3) the contents of (4) plaintiffs' electronic communications (5) using a device." *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 794–95 (N.D. Cal. 2022). Similarly, to plead a wiretapping claim under CIPA § 631(a), Plaintiffs must show that Microsoft "[1] willfully [2] attempt[ed] to learn the contents or meaning of a communication [3] in transit [4] over a wire." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192 (1978).[10] Plaintiffs allege so-called interception of actions, not communications, and do not allege interception while in transit.

1. Plaintiffs Fail to Allege that Microsoft Intercepted any Communication.

Plaintiffs do not allege they engaged in any traditional communications, like phone calls, but instead focus exclusively on the alleged collection of their "personal information and specific web activity." Compl. ¶ 1. In doing so, Plaintiffs conflate *actions* with *communications. See, e.g.*, *id*. ¶ 60 (describing a user's "selection of an article or video [they] would like to view" as a

[10] The first clause of Section 631(a), related to "intentional wiretapping," applies only to any "telegraph or telephone wire," which is not relevant here.

"communication"); *see also* ¶¶ 368, 374 (alleging "Plaintiffs website page visits, selections, bookings, appointment information, purchases and persistent identifiers" are communications). But actions are not "communications" under any ordinary reading of the term. As multiple courts have agreed, both the Wiretap Act and CIPA were intended to protect person-to-person communications, not website browsing. *See, e.g.*, *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1086 (N.D. Cal. 2018) (dismissing CIPA claim because "opening a webpage" is "not a communication with content"); *see also Zynga*, 750 F.3d at 1103 (amendments to the Wiretap Act focused on "electronic communications services" such as "the transfer of electronic messages, such as email, between computer users") (citation omitted). Because Plaintiffs have not plausibly alleged communications are at issue, their wiretap claims fail.

Even if Plaintiffs' actions were communications (and they are not), their wiretap claims would still fail because they do not allege facts plausibly showing that Microsoft collected the "*contents*" of any such "communication." CIPA and the Wiretap Act treat this issue the same way. *See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (2020). The "contents" of a communication are "any information concerning the substance, purport, or meaning of the communication." 18 U.S.C. § 2510(8); *see also Zynga*, 750 F.3d at 1104. Plaintiffs assert that Microsoft's alleged "collection of the universal resource locator ('URL') for each page of each website visited by an individual" constituted the collection of the "contents" of communications. *See* Compl. ¶¶ 61–65. But the Ninth Circuit disagrees. *See Zynga*, 750 F.3d at 1107–08 (URLs merely represent the "location of a webpage a user is viewing on the internet," not the "contents" of any communication"). And while *Zynga* left open the possibility that, *in some circumstances*, URLs revealing a person's search terms *could* include a person's communications, *id.* at 1108–09, none of the Plaintiffs here alleged that Microsoft collected their search terms or other input text through URLs. Because URLs are not "a person's intended message to another," *id.* at 1106, and because that is the only communication Microsoft allegedly collected, Plaintiffs do not

plausibly allege any contents of any communication, dooming their wiretap claims. *See also Cook*, 689 F. Supp. 3d at 70 ("movements and clicks" constitute "a record of . . . movements within a digital space," not any "communicative" content); *King v. Hard Rock Cafe Int'l (USA), Inc.*, No. 24-cv-01119, 2025 WL 1635419, at *4 (E.D. Cal. June 9, 2025) (dismissing CIPA claims where pixel allegedly collected "button clicks" and "URLs" related to hotel "booking information"); *Griffith v. TikTok, Inc.*, No. 23-cv-00964, 2024 WL 5279224, at *10 (C.D. Cal. Dec. 24, 2024) (similar); *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082 (C.D. Cal. 2021) (similar).

2. Plaintiffs Fail to Allege that Any Interception Occurred "In Transit."

Plaintiffs' wiretapping claims under both the federal and California law fail for the independent reason that Plaintiffs do not plausibly allege that Microsoft intercepted any communication of theirs "in transit," as both statutes require. *See Adler v. Community.com, Inc.*, No. 21-cv-02416, 2021 WL 4805435, at *3–4 (C.D. Cal. Aug. 2, 2021); *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868, 878 (9th Cir. 2002). Plaintiffs must allege that Microsoft acquired the contents of a communication during its transmission, not after it was received or stored by the website. *Id.*

Here, Plaintiffs offer only a conclusory assertion that the Xandr and UET pixels "intercepted" their communications "in transit." *See* Compl. ¶ 333. But Plaintiffs plead no facts to support this. Their "formulaic recitation of the elements" does not suffice. *See Twombly*, 550 U.S. at 555.

Moreover, the facts alleged are inconsistent with interception "in transit." Plaintiffs allege that the Xandr and UET pixels allow Microsoft to collect URLs and related data after Plaintiffs visited certain websites. *See, e.g.*, Compl. ¶¶ 61, 77. But as the Ninth Circuit has explained, when a user enters a URL or interacts with a website, the user's browser (the "client") sends a "GET request" to the website's server, which then responds by delivering the requested content. *See Zynga*, 750 F.3d at 1101–02. Any URLs collected utilizing these pixels necessarily occurred

after the website had received and responded to the user's request. *See id*.; *see also Griffith*, 2024 WL 5279224, at *10 (the "sequence" of transmission is determinative for interception claims), *appeal filed*, No. 25-553 (9th Cir. Jan. 28, 2025). For example, and as a matter of logic, to the extent that any URL reflected hotel booking information, Compl. ¶¶ 64–65, 200, that information had to have been selected by the user *before* the URL was generated for the URL to include it. Accordingly, any data collection through the URL, would have had to occur *after* the Plaintiff transmitted it to the website. Similarly, any cookie syncing or other data sharing with third parties would likewise have had to occur only *after* a Plaintiff interacted with a website. *See, e.g.*, Compl. ¶ 41 (explaining three-step cookie process occurring after a user lands on a website).

Thus, Microsoft could not plausibly have acquired any communication "in transit." Instead, any alleged collection occurred after the websites received Plaintiffs' requests. This defeats Plaintiffs' federal and California wiretap claims. *See Konop*, 302 F.3d at 878; *Griffith*, 2024 WL 5279224, at *10.

3. Plaintiffs' Wiretap Act Claim Fails Because the Website Operators Consented to Use of Xandr and UET.

The Wiretap Act permits the interception of communications where one party to the communication consents. *Nienaber v. Overlake Hosp. Med. Ctr.*, 733 F. Supp. 3d 1072, 1095 (W.D. Wash. 2024); 18 U.S.C. § 2511(2)(d). Plaintiffs allege that each of the websites were parties to their so-called communications. *See, e.g.*, Compl. ¶ 374 (alleging that Plaintiffs' "interactions ***with each website*** are electronic communications") (emphasis added). And they admit that the website operators, not Microsoft, installed the Xandr and UET pixels on their sites. *See* Compl. ¶ 15 (explaining "***website operators*** can integrate [pixels] into their websites") (emphasis added). Because the websites chose to deploy these services, they consented to Microsoft's alleged collection of data through them. *Rodriguez v. Google LLC*, No. 20-CV-04688, 2021 WL 2026726, at *6 (N.D. Cal. May 21, 2021) (dismissing Wiretap Act claim where "Google's alleged interceptions occurred with the consent of app developers").

Plaintiffs argue the "crime-tort" exception obviates website consent because they say that Microsoft created "profiles," and that this constitutes unlawful "use" of their data. But neither Microsoft's alleged collection nor its intended use of the data for advertising was in any way unlawful. "The focus [of the Wiretap Act crime-tort exception] is not upon whether the interception itself violated another law; it is upon whether the *purpose* for the interceptions—its intended use—was criminal or tortious." *Sussman v. Am. Broad. Companies, Inc.*, 186 F.3d 1200, 1202 (9th Cir. 1999) (citation omitted); 18 U.S.C. § 2511(2)(d); *see also In re Google Inc. Gmail Litig.*, No. 13-MD-02430, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014) (the exception applies only where the "primary motivation or a determining factor in [the interceptor's] actions has been to injure plaintiffs tortiously") (citation omitted).

Plaintiffs do not allege that Microsoft acted with "the purpose of facilitating some further impropriety, such as blackmail." *Sussman*, 186 F.3d at 1202. Instead, they allege Microsoft sought to generate revenue by providing more useful advertising to its website customers. *See, e.g.*, Compl. ¶ 230 (alleging that collection was "done both for Defendant's profit and for the profit of the Pixel Partners"). The crime-tort exception simply "cannot apply." *In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *18 n.13; *see also Lakes v. Ubisoft, Inc.*, No. 24-cv-06943-TLT, 2025 WL 1036639, at *7 (N.D. Cal. Apr. 2, 2025) (rejecting the crime-tort exception where defendant's motivation was "improv[ing] the effectiveness of its and Meta's advertising and marketing").[11]

[11] This case is nothing like the cases cited in Plaintiffs' Complaint. *Cf. Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021) (exception applied where defendant "associate[ed] . . . data with preexisting user profiles" even though users enabled a private browsing mode); *Marden v. LMND Med. Grp., Inc.*, No. 23-CV-03288, 2024 WL 4448684, at *3 (N.D. Cal. July 3, 2024) (exception applied where defendant "purposefully configured its website to intercept individually identifiable information about highly sensitive health issues"); *R.C. v. Walgreen Co.*, 733 F. Supp. 3d 876, 890, 901–02 (C.D. Cal. 2024) (exception applied where "private health information was rendered personally identifiable" because it was disclosed and associated with "active Facebook accounts").

4. The Court Should Dismiss Plaintiffs' Claims for Improper Use and Disclosure.

Both the Wiretap Act and CIPA prohibit use and disclosure of unlawfully intercepted communications. *See* 18 U.S.C. § 2511(c)–(d); Cal. Penal Code § 631. As explained, Plaintiffs do not allege facts showing that Microsoft unlawfully intercepted their communications. Therefore, they likewise have not alleged facts that Microsoft used or disclosed such intercepted communications, requiring dismissal of their use and disclosure claims. *See* Compl. ¶¶ 334, 377.

5. Plaintiffs Fail to Allege Aiding and Abetting Liability under CIPA.

Plaintiffs claim that Microsoft "aid[ed] in the wiretapping of [Plaintiffs'] communications by Partner Pixels" by allegedly sharing anonymous information with them. *See, e.g.*, Compl. ¶¶ 168, 252. Just as Plaintiffs have not alleged facts establishing that *Microsoft* unlawfully intercepted their communications, or that it did so while any communication was in transit, they likewise have not alleged facts establishing that any *third party* has done so. *See Cody v. Ring LLC*, 718 F. Supp. 3d 993, 1003 (N.D. Cal. 2024) (dismissing CIPA aiding and abetting claim where the plaintiff "fail[ed] to establish an underlying third-party violation"). There is nothing to aid and abet where there is no underlying unlawful conduct alleged. Indeed, the Complaint contains only sparse allegations regarding how third-party pixels even operate.

Regardless, Plaintiffs' allegations establish the opposite of aiding and abetting: Microsoft's only engagement with third party pixels consisted of "cookie syncing," i.e. attaching a random identifier to browsing data already collected, not the initial, simultaneous interception of communications that CIPA governs. *See, e.g.*, Compl. ¶ 291. Plaintiffs' conclusory allegations that Microsoft "aids" the partner pixels' alleged wiretapping—without any explanation of how Microsoft supposedly assisted these partner pixels with the interception of communications as opposed to later marketing activity—do not suffice. *See, e.g.*, *id.* ¶ 132.

C. Plaintiffs Fail to Allege that Microsoft Utilized a "Pen Register" in Violation of Cal. Pen. Code § 638.51(a).

California's pen register statute prohibits a person from "install[ing] or us[ing] a pen register" without a court order. A "pen register" is a "device or process that records or decodes" certain types of routing information "transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code. § 638.50(b). Plaintiffs allege that the Xandr and UET pixels are "pen registers" because they collect Plaintiffs' IP addresses and device information. Compl. ¶ 347.[12]

But Xandr and UET pixels cannot be "pen registers" because a "'pen register' is a 'device or process' that records *outgoing* information (e.g., the telephone number that is dialed)." *see* Compl. ¶¶ 344–45. In contrast, Microsoft allegedly collected *incoming* information, i.e., Plaintiffs' IP address, which would be akin to the telephone number associated with an incoming call. *See also* Cal. Penal Code § 638.50(b) (defining a pen register as recording or decoding "information *transmitted* by an instrument or facility") (emphasis added).

Beyond that, Plaintiffs' pen register claim fails for a more fundamental reason: California's pen register statute does not apply to ordinary commercial websites that do not send or receive person-to-person communications. The text and legislative history of the statute, like its federal analogue, conforms to common understanding of pen registers as devices that show "which people" are "communicating with one another and at what times." Assem. Com. on Public Safety, Analysis of Assem. Bill No. 929, CA, 2015-2016 Reg. Sess. at T; *see also United States v. New York Tel. Co*., 434 U.S. 159, 161 n. 1 (1977) (a "pen register" is a "device that records the [outgoing] numbers dialed on a telephone"). None of the websites at issue are communications services that facilitate person-to-person conversations, like phone lines. Pen

[12] As explained, although Plaintiffs allege collection of geolocation information in conclusory fashion, they do not allege this was collected from any of *them. See supra* at 5. In any event, whether Microsoft collected location information would not change the result under CIPA.

registers therefore cannot attach to them. *See also Sanchez v. Cars.com Inc.*, No. 24STCV13201, 2025 WL 487194, at *3 (Cal. Super. Ct. Jan. 27, 2025).

Similarly, by definition, a "pen register" must collect information *about a communication*. *See* Cal. Penal Code § 638.50(b) (a pen register records "information" about a communication, "but not the *contents of a communication*.") (emphasis added). As discussed above, *supra* 14–16, Plaintiffs do not plausibly allege they conveyed any such communication, and Plaintiffs tacitly concede this by bringing a pen register claim in the alternative to their wiretapping claim. *See* Compl. ¶ 347. However, because a pen register collects the non-content aspects of a *communication*, the absence of communications content destroys *both* Plaintiffs' wiretap and pen register claims. *See Sanchez*, 2025 WL 487194, at *3.

Adopting Plaintiffs' interpretation would mean that any person or company that receives an IP address—even the website itself, which cannot function without processing an IP—risks violating criminal law. California's pen register statute "did not, and does not, criminalize the process by which all websites" operate. *Casillas v. Transitions Optical, Inc.*, No. 23STCV30742, 2024 WL 4873370, at *4 (Cal. Super. Ct. Sept. 9, 2024); *Licea v. Hickory Farms LLC*, 2024 WL 1698147, at *2 (Cal. Super. Ct. Mar. 13, 2024).

D. The Rule of Lenity Requires Interpreting the Wiretap Act and CIPA Narrowly.

The Wiretap Act and CIPA are criminal statutes that carry the weight of possible imprisonment. *See* 18 U.S.C. § 2511(4)(a); Cal. Penal Code §§ 631(a), 638.52(c). Their language must be "clear and definite" to "give fair notice" of prohibited conduct. *See Nosal*, 676 F.3d at 863. When in "doubt," courts "must choose the interpretation least likely to impose [unintended] penalties." *Id.* at 863 (cleaned up); *see also United States v. Lanier*, 520 U.S. 259, 266 (1997) (requiring resolution of "ambiguity in a criminal statute as to apply it only to conduct clearly covered").

A plain reading of the Wiretap Act and CIPA does not lead to Plaintiffs' position that routine online advertising activities creates criminal liability for millions of market participants. Nor does the legislative history support imposing such sweeping liability. Neither statute mentions online browsing activity, pixels, or cookies. Nor does California's pen register statute, instead repeatedly referencing "telephone lines" and "number[s]." *See, e.g.*, Cal. Pen. Code § 638.52(1), (3), (5). And other California laws, passed after both the Wiretap Act and CIPA, explicitly *authorize* the collection of online browsing information. *See supra* at 12. The California legislature has expressed the view that CIPA does not apply to these routine commercial transactions. *See supra* at 4. Under these circumstances, no company engaged in online advertising (of which there are "thousands" if not "millions," Compl. ¶ 220), can be said to have been on notice that their conduct violates criminal law.

Legislatures do not criminalize conduct through innuendo and vagueness. Instead, given the "absence of an express textual provision or an indication of legislative intent" supporting Plaintiffs' position, the "rule of lenity applies" and Plaintiffs' claims "should be dismissed." *See Vita v. New England Baptist Hosp.*, 494 Mass. 824, 848, 850 (2024) (citations omitted). Any other conclusion would improperly and "unintentionally turn ordinary citizens into criminals." *Nosal*, 676 F.3d at 863; *Harrott v. County of Kings*, 25 P.3d 649, 659 (Cal. 2001); *see also In re DoubleClick Inc. Priv. Litig.*, 154 F. Supp. 2d 497, 512–13 (S.D.N.Y. 2001) (refusing to interpret the federal Wiretap Act to criminalize "access[ing] cookies on users' hard drives").

E. Plaintiffs Fail to State a Claim for Unjust Enrichment.

Plaintiffs claim they are entitled to restitution on the basis that Microsoft "unlawfully trafficked" in their data "without their consent for substantial profits." Compl. ¶¶ 355–56. This does not state a claim for unjust enrichment.[13]

[13] Plaintiffs purport to bring this claim under California law on behalf of a nationwide class, but California unjust enrichment law does not apply extraterritorially, so Plaintiffs cannot bring such a claim on behalf of non-California residents.

First, unjust enrichment "is not a cause of action, just a restitution claim." *See Low*, 900 F. Supp. 2d at 1031 (collecting cases); *see also* 1 WITKIN, SUMMARY 11TH CONTRACTS § 1050 (2025) ("There is no separate cause of action in California for unjust enrichment.") (collecting cases).

Second, when courts do allow independent unjust enrichment claims to proceed, they do so by re-interpreting the claim as one for restitution under a quasi-contract theory—but there is no privity here. *ESG Cap. Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016). Plaintiffs do not allege privity or even interaction with Microsoft, and do not point to purported promises made by Microsoft to Plaintiffs regarding the conduct at issue. A quasi-contract claim could not apply. *See Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1096 (N.D. Cal. 2022) (dismissing unjust enrichment claim in a wiretap case when plaintiff failed to allege a misrepresentation or omission by defendant, as required to state a claim for restitution).

Third, unjust enrichment requires Microsoft to have "unjustly retained a benefit at the plaintiff's expense." *ESG Cap. Partners*, 828 F.3d at 1038. Plaintiffs do not allege any unjust conduct by Microsoft. "[I]t is not enough that" the Plaintiffs allegedly provided a benefit to Microsoft (which Microsoft does not concede); Plaintiffs "must also allege that [Microsoft] unjustly secured that benefit through qualifying conduct." *Russell v. Walmart, Inc.*, 680 F. Supp. 3d 1130, 1133 (N.D. Cal. July 5, 2023) (citations omitted). For example, Plaintiffs have not alleged any "mistake, fraud, coercion, or request" that would typically undergird a finding of "unjust" conduct. *Id.* (citations omitted); *see also Hammerling*, 615 F. Supp. 3d at 1096; *Dinosaur Dev., Inc. v. White*, 216 Cal. App. 3d 1310, 1316 (1989). To the contrary, Microsoft and its third-party partners are transparent about the practices challenged in the Complaint. *See supra* at 12. And for the same reasons Plaintiffs fail to show injury-in-fact, *see supra* 7–11, they fail to show that any enrichment to Microsoft was "at their expense."

Fourth, Plaintiffs have not pleaded they lack an adequate remedy at law, a fundamental prerequisite for their equitable unjust enrichment claim. *Chiulli v. Am. Honda Motor Co.*, 690 F. Supp. 3d 1038, 1062 (N.D. Cal. 2023). Indeed, they seek money damages. *See* Compl. at 78. This bars them from seeking equitable relief. *See Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020) (affirming dismissal of claims for equitable restitution where the plaintiff "requested in damages to compensate her for the same past harm"); *Vance v. Google LLC*, No. 20-CV-04696, 2024 WL 5011611, at *7 (N.D. Cal. Dec. 5, 2024) (similar).

F. The Statutes of Limitations Bar Plaintiff Mason's Claims.

Plaintiff Mason alleges he visited the Plushcare website "in or about February 2021."[14] Compl. ¶ 289. The limitations periods for his claims range from one to two years. *See* Cal. Civ. Proc. Code § 335.1; Cal. Civ. Proc. Code § 340; 18 U.S.C. § 2520(e); Cal. Civ. Proc. Code § 339. Yet he filed his Complaint here in April 2025, more than four years after the alleged violation. *See id.* His claims are time-barred, requiring dismissal. *See, e.g., Brodsky*, 445 F. Supp. 3d at 136–39 (N.D. Cal. 2020) (dismissing CIPA claims as time-barred); *Al-Ahmed v. Twitter, Inc.*, 648 F. Supp. 3d 1140, 1157 (N.D. Cal. 2023) (dismissing ECPA claim as time-barred); *Wu v. Sunrider Corp.*, 793 F. App'x 507, 509 (9th Cir. 2019) (affirming dismissal of unjust enrichment claim as time barred).

CONCLUSION

For the foregoing reasons, Microsoft respectfully requests that the Court dismiss the Complaint with prejudice for lack of subject matter jurisdiction under Federal Rule of Civil Procedure 12(b)(1) and/or failure to state a claim for relief under Federal Rule of Civil Procedure 12(b)(6).

[14] Microsoft did not acquire Xandr until June 2022, after Mr. Mason's alleged visit to Plushcare. *See* Microsoft, *Microsoft to Acquire Xandr to Accelerate Delivery of Digital Advertising and Retail Media Solutions* (Dec. 21, 2021).

DATED: June 23, 2025

By: */s/ James G. Snell*

James G. Snell (pro hac vice)
PERKINS COIE LLP
3150 Porter Drive
Palo Alto, California 94304-1212
Phone: (650) 838-4300
E-mail: JSnell@perkinscoie.com

Nicola Menaldo, WSBA No. 44459
Jordan C. Harris, WSBA No. 55499
PERKINS COIE LLP
1301 Secon Avenue, Suite 4200
Seattle, WA 98101-3099
Phone: 206.359.8000
Fax: 206.359.9000
Email:NMenaldo@perkinscoie.com
Email: JordanHarris@perkinscoie.com

Justin Potesta (pro hac vice)
PERKINS COIE LLP
405 Colorado Street, Suite 1700
Austin, TX 78701
Tel: (737) 256.6137
jpotesta@perkinscoie.com

Attorneys for Defendant
Microsoft Corporation

LCR 7(e) Certification

I certify that this memorandum contains 8,297 words, in compliance with the Local Civil Rules.

/s/ James G. Snell